Application Service Provider Privacy & Security Policies

Access	Access to the data in ABELMed is controlled by Windows accounts and permissions, attached to role based security within the application. Physical Access to the datacenter is controlled by security guard and smart card and is restricted.
Authorization	The ABELMed Authorization Manager is used to select the security mode, add staff members to the system and assign them access privileges (typically by role) to the ABELMed information they need to do their jobs effectively. One user per subscriber/practice is granted access to the Authorization Manager. This user has the ability to alter existing roles and privileges and to define new roles and privileges.
Authentication	Authentication is controlled by Windows security (Kerberos v5 / NTLM)
Audit	Auditing consistent with the CCHIT requirements is provided through a combination of Microsoft Windows auditing and logging (enforced and controlled by Windows Group Policy) combined with ABELMed logging within the application.
Secondary Uses of Data	ABEL Medical Software Inc. will not use or exploit in any way any such patient and physician data, including but not limited to data containing personally identifiable information or data that is in aggregate form, except to provide services to the Subscriber.
Data Ownership	Patient and physician data is owned by the Subscribers. ABEL Medical Software Inc. will not use or exploit in any way any such patient and physician data, including but not limited to data containing personally identifiable information or data that is in aggregate form, except to provide services to the Subscriber. Data will be returned to the subscriber on written request, and backup copies destroyed.